40th Annual Election Law Seminar for County Election Officials

Hash Validation

What is Hash Validation?

“Hash validation is a security process designed to ensure data integrity. It is an independent check and validation that verifies installed firmware and/or software exactly matches the version of firmware and/or software that has been tested and approved by an accredited voting system test laboratory (VSTL) and certified by the US Election Assistance Commission (EAC).”

Why is Hash Validation Important?

“Hash validation provides an integrity check which verifies the firmware and/or software installed on the equipment is the certified version(s). Hash validation, effective chain of custody procedures, logic and accuracy testing and physical security measures are essential to conducting a transparent and trustworthy election. ”

How Does the Hash Validation Process Work?

High-Level Example of How the Hash Validation Process Works

Hashing Certified Version of ES&S FW/SW *at Test Lab by VSTL*

- Operating System Export Files
- FIPS 140-2 Certified Hash Algorithm (SHA256)
- VSTL Generates Trusted Hash Files
- EXAMPLE HASH OUTPUT: ac49e74434a64c2d 47aa129bef83f2048
- Certified hash output is securely stored at customer site.
- *Matching hash output verifies that the FW/SW at the customer site is unaltered from the certified version.*

Hashing ES&S FW/SW Installed *at Customer Site*

- Operating System Export Files
- FIPS 140-2 Certified Hash Algorithm (SHA256) Customer Generates Hash Files
- EXAMPLE HASH OUTPUT: ac49e74434a64c2d 47aa129bef83f2048
- *Matching hash output verifies that the FW/SW at the customer site is unaltered from the certified version.*

FIPS 140-2 Compliant – SHA256 Algorithm – Ubuntu 16.04.1

- FIPS

- stands for the Federal Information Processing Standard established by the National Institute of Standards and Technology (NIST), for use in computer systems for the purpose of ensuring security and interoperability through data encryption.

- SHA256
  - (Secure Hash Algorithm 256) is a hashing algorithm used by certification authorities to sign certificates. SHA256 is used to convert the EXPORT files into a fixed size string file (Hash File).

- Ubuntu 16.04.1
  - is FIPS 140-2 validated and compliant third-party software used to compare the Trusted Hash File to the Hash File exported from the voting system firmware.

SECURITY FACT

The ES&S Hash Validation process requires a Verification PC (Ubuntu)
- Verification PC Setup guide is provided with the Technical Data Package (TDP) documents for County to follow in the process of setting up a PC
- County provides/sends a laptop to ES&S for wiping and installation of Ubuntu 16.04.1
- County purchases a laptop from ES&S that has Ubuntu 16.04.1 preinstalled

SECURITY FACT

The ES&S Hash Validation process requires the ES&S Verification Pack files provided to customer(s) on a DVD as part of the hash validation process set forth in ES&S' TDP.

SECURITY FACT

The ES&S Hash Validation process requires ES&S USB flash drives.

Step 1: Prepare USB Media

- QUALIFY – Initialize EQC USB and copy contents of EQC folder located in Verification Pack to USB flash drive.
- ELECTION – Initialize ELECTION USB and copy contents of (specific equipment) Election Definitions folder located in Verification Pack to USB flash drive.
- SCRIPTS – Initialize SCRIPTS USB and copy specific files from Verification Scripts folder to USB flash drive.
- EXPORT – Initialize and format Firmware EXPORT USB to be used to export files from voting device(s).

Step 2: Create and Export Validation Media

Step 3: Verify the Firmware Export (Current)

- Initialize Verification PC
  - Boot the Verification PC and log in with secure user credentials

- Identify and Load Storage Devices
  - SCRIPTS – Insert Scripting USB Flash Drive
    - Enter Linux command to list device and partitions file names
  - EXPORT – Insert Firmware Export USB Flash Drive
    - Enter Linux command to list device and partitions file names
    - Enter Linux commands to load storage devices

- Execute Verification Scripts
  - Enter Linux commands to create temporary verification directory and load Firmware Export files
  - Enter Linux command to compare firmware to the Trusted Hash File

- If the (i.e. DS200) hash matches the Trusted Hash File, the following message will be displayed: DS200 firmware matches Trusted Hash File. Hash File, DS200-Identification_Hash.txt, copied to output.
-
- DS200-Identification is the name used to identify the DS200 for which the verification reports were generated.

Step 3: Verify the Firmware Export (EVS 6200+)

- Initialize Verification PC
  - Boot the Verification PC and log in with secure user credentials

- Identify and Load Storage Devices
  - SCRIPTS – Insert Scripting USB Flash Drive
  - EXPORT – Insert Firmware Export USB Flash Drive

- Execute Verification Scripts
  - Launch terminal window
  - Enter Linux command to compare firmware to the Trusted Hash File

- If the hash matches, the following output will display:
  - Firmware validation results: * SerialNumber: MATCH Syncing file system. Please wait...The script completed. You may now remove both the Scripting USB flash drive and the Firmware Export USB flash drive.